The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB GOVERNMENT'S RESPONSE TO SECOND MOTION TO SUPPRESS AND REQUEST FOR *FRANKS* HEARING **FILED UNDER SEAL**

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton and Andre Penalver, Assistant United States Attorneys for said District, and Keith A. Becker, Trial Attorney, hereby files this response to the Defendant's Second Motion to Suppress Evidence and Motion for *Franks* Hearing. For the reasons stated herein, the defendant's motion should be denied.

I. INTRODUCTION

The defendant's second suppression motion again seeks to suppress IP address information and other computer-related evidence obtained through deployment of a court-authorized Network Investigative Technique ("NIT") in an effort to identify registered users, like Michaud, who accessed child pornography on Website A, while they were concealing their identity and location through use of the Tor anonymity network. His motion is without merit.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

As discussed below, use of the NIT was authorized by a valid search warrant upon finding of probable cause and Michaud does not–and cannot–produce sufficient evidence to show that the warrant is properly subject to challenge under the "*Franks*" analysis. The sum total of Michaud's "*Franks*" argument is that it may have been theoretically possible for a user to access Website A without the intent to view child pornography. Considering, as the court must, the totality of the circumstances, including reasonable inferences, probable cause existed to support the requested warrant.

Moreover, the NIT warrant and application complied with the requirements of the Fourth Amendment. It set forth with particularity the places to be searched and the specific, limited set of evidence to be seized from users to whom it applied. The warrant was therefore sufficiently particular and its scope–in terms of the items to be seized–was both extremely limited and specifically targeted to the identifying information sought via the warrant. While Michaud attempts to re-define the concept of scope under the Fourth Amendment to suit his argument that the warrant was overbroad because it applied to many users of Website A, an analysis of that concept as defined by the Supreme Court shows that Michaud's "general warrant" argument also fails.

II. FACTS

Pertinent background of the investigation is set forth in the government's response to the defendant's first motion to suppress, incorporated herein by reference. Dkt. 47 at 2-8. A description of Website A and its content is contained in paragraphs 11-27 of the NIT warrant affidavit. One of the many components of the website that is described in the affidavit is the site's main page. Michaud's primary *Franks* argument pertains to the description of images that were present on the main page of the website.

The NIT search warrant affidavit describes images contained in the site's logo on the main page of the website. Specifically, paragraph 12 of the NIT search warrant affidavit states that "on the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent females with their legs spread apart." Dkt. 47, Ex. 1, ¶ 12. A printout of the main page and that logo as of February 3, 2015, is attached as Exhibit 1. Paragraph 11 of the NIT search warrant affidavit articulates that the website had been reviewed by FBI special agents between September 16, 2014, and February 3, 2015, at its prior Uniform

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Resource Locator ("URL").[1] A footnote to that paragraph articulated that the affiant accessed Website A on February 18, 2015, after observing that the website's URL or web address had apparently been moved by its administrator, and "determined that its content had not changed." *Id*., p. 14-15, n. 3. The description of the logo images in Paragraph 12 of the NIT search warrant affidavit is correct as of February 18, 2015. At the time, the website had not been yet seized by law enforcement agents, nor had the site administrator been apprehended.

In the evening of February 19, 2015, the FBI executed a search at the Naples, FL, home of the website administrator and apprehended him. Dkt. 47, Ex. 1, p. 23, ¶ 30. Postings by the administrator of Website A indicate that during the day of February 19, 2015, before he was apprehended, the administrator altered the site logo and the images that appeared on it. A printout that shows the site logo as of its alteration by the administrator on February 19, 2015, is attached as Exhibit 2. The administrator replaced the two images previously depicted on the site logo with a single image depicting a prepubescent female, wearing a short dress and black stockings, posed sitting reclined on a chair with her legs crossed, in a sexually suggestive manner. *Id*. Pertinent text described on the logo–i.e., the terms, "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview," which the affidavit explained pertain to image distribution, remained the same as on the prior logo. *Compare* Dkt. 41, Ex. 1, p. 13, ¶ 12 *with* Ex. 2.

The NIT warrant was sworn to and authorized at 11:45 a.m. on February 20, 2015. Dkt. 47, Ex. 1, Warrant. The warrant affidavit articulated that it included "only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation." *Id*., p. 2, ¶ 3. The administrator's February 19, 2015, alteration of the site logo, just before the warrant was authorized, is not referenced in the warrant affidavit.

III. ARGUMENT

In support of his motion to suppress and request for a *Franks* hearing, Michaud contends that the affiant falsely described images on the main page of the website, takes issue with statements made and conclusions drawn by the affiant within the warrant affidavit, and claims

[1] A "URL" is sometimes referred to a as "web address." On the open internet, www.cnn.com is an example of a URL. On the Tor network, a URL consists of a series of 16 algorithm-generated characters, followed by the suffix ".onion"–i.e., an59rhe329ht549h.onion.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

that statements in the warrant and application regarding the location of the search were misleading. All of these arguments are unavailing. As to the first two theories, the sum total of Michaud's probable cause/*Franks* argument is that he contends it was theoretically possible that a user could have accessed Website A without an intent to view child pornography. But the government was not required to show definitely that every visitor to Website A intended to access child pornography. The government merely had to show that it was reasonably likely that persons who logged onto Website A did so for that purpose. This was indeed a reasonable inference to be drawn from the totality of the circumstances, and since there was probable cause to believe visitors to Website A were seeking child pornography even without the purported misrepresentations Michaud has identified, his *Franks* argument fails for lack of materiality. In addition, Michaud's contentions regarding the location of the search are contradicted by the plain language of the warrant, application, affidavit and attachments. Accordingly, the Court should deny Michaud's motion.

A. *Franks* Allegations Require a Substantial Preliminary Showing and Materiality.

"[T]o be entitled to a *Franks* hearing, the defendant must first make a non-conclusory and substantial preliminary showing that the affidavit contained actual falsity [or an omission], and that the falsity either was deliberate or resulted from reckless disregard for the truth." *United States v. Prime*, 431 F.3d 1147, 1151 n.1 (9th Cir. 2005) (internal quotations omitted); *see also United States v. Meling*, 47 F.3d 1546, 1553 (9th Cir. 1995) (extending the analysis to false inclusions or omissions). A defendant must also demonstrate that the alleged falsity or omission is material. *United States v. Chavez-Miranda*, 306 F.3d 973, 979 (9th Cir. 2002). A false statement or omission is not material unless the affidavit, purged of its defects, would be insufficient to support a finding of probable cause. *Meling*, 47 F.3d at 1553; *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000). For materiality "the pivotal question is whether an affidavit containing the omitted material would have provided a basis for a finding of probable cause." *Chavez-Miranda*, 306 F.3d at 979.

This standard was established by *Franks v. Delaware*, 438 U.S. 154, 155-56, 170-72 (1978), where the Supreme Court stressed that there is a presumption of validity with respect to a search warrant affidavit. As such, the Court required a defendant's showing to be more than

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

conclusory and the claim must contain allegations of deliberate falsehood. *Id.* at 171. Those allegations must be accompanied by an offer of proof, and affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained before a hearing is granted. *Id*. Allegations of negligence or innocent mistake are insufficient. *Id.* In *Franks* and subsequent cases, the Supreme Court has been "careful . . . to avoid creating a rule which would make evidentiary hearings into an affiant's veracity commonplace, obtainable on a bare allegation of bad faith. It crafted, therefore, a rule of very limited scope." *United States v. Chesher*, 678 F.2d 1353, 1360 (9th Cir. 1982).

In *Meling*, for example, the defendant alleged that the affidavits supporting wiretaps contained some knowing and misleading statements along with some unknowing omissions. The intentional falsehoods included omitting the informant's old convictions for forgery and fraud and the agents' knowledge that the informant was motivated, in part, by a big financial reward. The same informant also had another recent felony conviction and a commitment to a mental institution, information that also was omitted from the affidavit. The *Meling* Court noted that "[f]or whatever reason, this information was not contained in the FBI's rap sheet. Defendant disbelieves the FBI, but that disbelief does not amount to the substantial showing required under *Frank*s." 47 F.3d at 1554; *see also United States v. Miller*, 753 F.2d 1475, 1478 (9th Cir. 1985) ("it might have been prudent for the federal agents to check on [an informant's] background and criminal record, but their failure to do so is not reckless disregard."). The court also held that the requested *Franks* hearing was properly denied because the omitted information was not material. Specifically, the court found that even if the information about the informant's forgery conviction and his financial motivation for coming forward had been added to the affidavits, it would not have eliminated probable cause. *Id.* at 1554-56.

B. Michaud Fails to Demonstrate any Intentional or Reckless Falsehoods in the Affidavit, Nor Has He Made the Requisite Showing of Materiality.

Applying these principles, it is clear that Michaud fails to make the requisite substantial preliminary showing to warrant a *Franks* hearing. First, Michaud fails to make the necessary showing of a deliberate or reckless material falsehood or omission, and his claim lacks anything close to a sufficient offer of proof. For example, he proffers no evidence that any purported omission of information about the administrator's change to the home page image just prior to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

authorization was even intentional, much less deliberate or reckless. The affidavit indicated that the site had been reviewed on February 18, 2015, Dkt. 47, Ex. 1, p. 14-15, n.3, before the administrator altered the site logo, and that the affidavit included "only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation," *Id*., p. 2, ¶ 3. While it might have been better has the affiant reviewed the website the day he sought the warrant (February 20, 2015), "[m]ere negligence in checking or recording the facts relevant to a probable-cause determination is not sufficient to warrant a *Franks* hearing." *United States v. Burnes*, 816 F.2d 1354, 1358 (9th Cir. 1987) (citation and quotations omitted). Similarly, a "good faith mistake" by the affiant will not invalidate the warrant. *United States v. Botero*, 589 F.2d 430, 433 (9th Cir. 1978).

To the extent that the lack of reference to the administrator's minor alteration of the site logo just before the warrant's authorization can be viewed as an omission, it was nothing more than an unintentional oversight. Even assuming the information pertaining to the change in the home page images consisted of an intentional or reckless false statement or omission, then, like the omitted information in *Meling*, this information simply was not material to the finding of probable cause. Had the purportedly omitted information been included in the affidavit–i.e., that the images on the site's main page were as described in the warrant affidavit between September 16, 2014 and February 19, 2015, but were altered by the administrator on February 19, 2015, the addition of that information into the warrant would not have defeated probable cause as will be discussed. Accordingly, the Court should deny Michaud's motion and request for a *Franks* hearing on the issue of the home page images.

1. The NIT Warrant Affidavit Established Probable Cause.

The NIT warrant affidavit amply supported a finding of probable cause, even when the information regarding the administrator's alteration of the site logo just prior to authorization is included. The 31-page NIT search warrant affidavit, sworn to by a veteran FBI agent with 19 years of federal law enforcement experience and specialized training and experience investigating the sexual exploitation of children, comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist law enforcement in identifying registered site users who were utilizing anonymizing technology to expose children to ongoing and pervasive sexual exploitation. Ex. 1, p. 1, ¶ 1. The description of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

the images visible on the site home page was but one component of that showing. The alteration to the images by the site administrator the day before the warrant was obtained is simply not material to probable cause.

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas v. United States*, 517 U.S. 690, 696 (1996). It is a fluid concept that focuses on "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quotation marks omitted). The task of a judge evaluating a search warrant application "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* at 238.

Probable cause requires "only the probability, and not a prima facie showing, of criminal activity." *Id.* at 235. "Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a 'commonsense, practical question,'" for which "[n]either certainty nor a preponderance of the evidence is required." *Id.* at 246; *see also United States v. Kelley*, 482 F.3d 1047, 1051-52 (9th Cir. 2007), and *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006). Indeed, "[f]inely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision." *Gates*, 462 U.S. at 235. In *Kelley*, the Ninth Circuit specifically emphasized that "locations such as computers can be searched for evidence of a crime even if there is no probable cause for arrest, or a prima facie showing of criminal activity, let alone proof sufficient to prosecute a criminal case beyond a reasonable doubt, or even to prevail under the civil burden that it is more likely true than not that he knowingly received or possessed child pornography." 482 F.3d at 1055. The NIT affidavit, supplemented with the information regarding the administrator's alteration to the site's home page, clearly established a fair probability that the use of the NIT would collect evidence of a crime for all registered users who logged onto Website A.

As the NIT affidavit explained, users who wished to access Website A were required to register an account, accept registration terms, and create a username and password before they

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

could access the site. Dkt. 47, Ex. 1, pp. 14-15, ¶¶ 12-14. Upon registration, all of the sections, fora, and sub-fora were observable. *Id.*, p. 15, ¶ 14. The vast majority of those sections were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. *Id.*, pp. 15-16, ¶14. The affidavit described in graphic detail particular child pornography that was available to all registered users of Website A, pornography which depicted prepubescent females, males, and toddlers being subjected to sexual abuse and exploitation by adults. *Id.*, pp. 17-18, ¶ 18. The affidavit accurately stated that "the entirety of [Website A was] dedicated to child pornography" and further specified a litany of site sub-fora which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id.* pp. 20-21, ¶ 27.

It is unlawful to access any computer disk–such as a website's computer server–with the intent to view child pornography, or to attempt to do so. 18 U.S.C. § 2252A(a)(5)(b). Accordingly, among other offenses, any user of Website A who accessed the site, or attempted to, with that intent would be guilty of that crime. To that end, the veteran NIT affiant affirmatively articulated that there was "probable cause to believe that . . . any user who successfully accesse[d]" the website had, at a minimum, "knowingly accessed with intent to view child pornography, or attempted to do so." Dkt 47, Ex. 1 p. 13, ¶ 10. The affiant drew this conclusion in light of the "numerous affirmative steps" required for a user to find and access Website A, which made it "extremely unlikely that any user could simply stumble upon" the site "without understanding its purpose and content." *Id.*, pp. 12-13, ¶ 10.

The Ninth Circuit has repeatedly held that "a magistrate may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found," *United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990) (quoting *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987)), including in child pornography cases. *See, e.g., United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000) (finding affidavit that included statements based on affiant's training and experience regarding child pornography trafficking and storage provided substantial basis for probable cause determination). Moreover, officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person." *United States v.*

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Hernandez, 313 F.3d 1206, 1210 (9th Cir. 2002) (quoting *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (evaluating factors supporting reasonable suspicion)).

The affiant's assessment that it was "extremely unlikely" a visitor to Website A would be ignorant of its content—and the magistrate's reasonable reliance upon that conclusion—was overwhelmingly supported by information articulated within the warrant. Website A was no ordinary, run-of-the-mill website that any unknowing person could stumble upon with a Google search, let alone access.[2] Rather, because the website operated on Tor, a user first had to connect to the Tor network and find the site, which required a user to obtain its lengthy, alphanumeric web address. Dkt. 47, Ex. 1, p. 12, ¶10. That user "might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location"–such as from a Tor "hidden service" page dedicated to pedophilia and child pornography, which contained a section with links to Tor hidden services that contain child pornography–including Website A. *Id.*

Moreover, the affiant stated that upon arrival at the site's main page before logging in, a user saw "to either side of the site name . . . two images depicting partially clothed prepubescent females with their legs spread apart." *Id*., p. 13, ¶ 12. Under a *Franks* analysis, the affidavit would be supplemented to articulate that the images described in the warrant were present on the main page of the site between September 16, 2014, and February 19, 2015, and that on February 19, 2015, the administrator altered the logo and replaced the two images previously depicted on the site logo with a single image depicting a prepubescent female, wearing a short dress and black stockings, posed sitting reclined on a chair with her legs crossed, in a sexually suggestive manner.[3] Whether the homepage contained a single photograph of a sexually posed child or two such photographs is completely immaterial to the probable cause showing.

---

[2] Michaud points the court to the search engine at https://ahmia.fi to contend that it is possible to search the Internet for information about Tor hidden services. That website has a "[c]ontent filtering policy" that states, "[w]e are removing each page which contains any child abuse from this search index" and provides a mechanism that users can report sites that contain child exploitation material. *See* https://ahmia.fi (last visited December 21, 2015). Michaud presents no evidence to show that any search run on that website would have obtained the web address for Website A.

[3] In his motion, Michaud describes the image more generically and contends that it is "apparent" that the child is not prepubescent. Dkt. 65, p. 4. Even a cursory review of the picture reveals that contention to be dubious.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The text underneath those suggestive images of prepubescent girls–"[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview"–which was carried over onto the new logo and indicated the site's dedication to image distribution. *Id*., p. 13, ¶ 12. The affiant stated that, "[b]ased on [his] training and experience, [he] know[s] that: 'no cross-board reposts' refers to a prohibition against material that is posted on other websites from being 're-posted' to the site and '.7z' refers to a preferred method of compressing large files or sets of files for distribution." *Id.*, p. 13, ¶ 12. And when viewed in conjunction with images displayed on the home page, it is reasonable to infer the images being distributed were child pornography. The site's registration terms also contained numerous indications that the site pertained to illicit activity–repeatedly warning prospective users to be vigilant about their security and the potential of being identified. *Id.*, pp. 14-15, ¶ 13. The issuing magistrate could accordingly have reasonably drawn an inference that any user who successfully found Website A was aware of its purpose and content.

The full, documented content of the website, as described in the affidavit, made it evident that the site's primary purpose was to advertise and distribute child pornography. Courts have routinely held that membership to a child pornography website, even without specific evidence of suspect downloading child pornography, provides sufficient probable cause for a search warrant because of the commonsense, reasonable inference that someone who has taken the affirmative steps to become a member of such a website would have accessed, received or downloaded images from it. *See Gourde*, 440 F.3d at 1070 (finding sufficient probable cause for residential search where defendant paid for membership in a website that contained adult and child pornography; noting reasonable, common-sense inference that someone who paid for access for two months to a website that purveyed child pornography probably had viewed or downloaded such images onto his computer); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005) (finding probable cause where purpose of the e-group "girls12-16" was to distribute child pornography; noting "[i]t is common sense that an individual who joins such a site would more than likely download and possess such material"); *United States v. Shields*, 458 F.3d 269 (3rd Cir. 2006) (finding probable cause where defendant voluntarily registered with two e-groups devoted mainly to distributing and collecting child pornography and defendant used suggestive email address); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) ("[I]t is common sense that a person who voluntarily joins a [child pornography] group . . . , remains a member of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

the group for approximately a month without cancelling his subscription, and uses screen names that reflect his interest in child pornography, would download such pornography from the website and have it in his possession."); *United States v. Hutto*, 84 Fed. Appx 6 (10th Cir. 2003) (affidavit sufficient to show probable cause where defendant became a member of a group whose obvious purpose was to share child pornography, and the images were available to all group members); *but see United States v. Falso*, 544 F.3d 110 (2nd Cir. 2008) (suppressing evidence from residential search for lack of probable cause where defendant was never accused of actually gaining access to the website that contained child pornography, there was no evidence that the primary purpose of the website was collecting and sharing child pornography, and defendant was never said to have ever been a member or subscriber of any child pornography site).[4] Here, like *Gourde*, the reasonable inference that the registered Website A users, at a minimum, accessed the site, or attempted to do so, with the intent to view child pornography easily meets the "fair probability" test.

2. The Possibility of Alternate Inferences Does Not Defeat Probable Cause.

Outside of his argument about the website's home page, the rest of the arguments that Michaud characterizes as "*Franks*" arguments are actually just argument about what weight the Court should attach to information and assessments the affiant included based on the evidence presented in the warrant and the affiant's training and experience. For example, Michaud takes issue with the affiant's assessment that the website was "dedicated to child pornography," Dkt. 47, Ex. 1, pp. 20-21, ¶ 27;[5] criticizes the significance of the affiant's description of the text contained underneath those suggestive images of prepubescent girls on the website's main page; and disagrees with the affiant's assessment that accessing Website A required "numerous affirmative steps" that made it "extremely unlikely that any user could simply stumble upon" the

---

[4] All of those cases evaluated probable cause before 18 U.S.C. § 2252A(a)(5)(B) was amended to make it unlawful to knowingly access a computer disk with intent to view child pornography, compare 18 U.S.C. § 2252A(a)(5)(B)(effective July 27, 2006) with 18 U.S.C. § 2252A(a)(5)(B)(effective October 8, 2008), making this case even stronger in terms of probable cause.

[5] Michaud claims that Website A advertised itself as a "chat forum." Dkt. 65, p. 8. Although there was a chat service contained within Website A, the warrant affidavit explained that the chat service contained on Website A that Michaud mentions was used to disseminate child pornography. *Id.*, pp. 19-20, ¶¶ 23-25. In fact, the affiant articulated multiple specific examples of child pornography distributed through the site's chat service. Dkt. 47, Ex. 1, p. 20, ¶ 25.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

site "without understanding its purpose and content." *Id.*, p. 12-13, ¶ 10. Michaud's disagreement with the affiant's description of the facts or inferences to be drawn from those facts in light the affiant's training and experience, however, does not an omission or falsehood make.

While Michaud is certainly entitled to argue about whether or not those facts and assessments, considering the totality of the circumstances, supported probable cause—and he has tellingly not directly challenged the affidavit's probable cause showing—he is not entitled to a *Franks* hearing just because he baldly characterizes information articulated in the warrant as "misleading." Moreover, the "omission rule [under *Franks*] does not require an affiant to provide general information about every possible theory, no matter how unlikely, that would controvert the affiant's good-faith belief that probable cause existed for the search." *United States v. Craighead*, 539 F.3d 1073, 1081 (9th Cir. 2008). As to these issues, Michaud fails to make any specific, or supported, allegations of actual intentional or deliberate falsehoods. Those allegations do "not amount to the substantial showing required under *Frank*s." 47 F.3d at 1554. "To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks v. Delaware*, 438 U.S. 154, 171 (1978). Michaud's remaining "*Franks*" arguments are conclusory, and merely the equivalent of a cross-examination of the affiant. That does not justify a hearing.

None of these arguments, even if accepted as true, are material to the issue of probable cause. The sum total of Michaud's argument is that it was theoretically possible that a user may have accessed Website A without intent to view child pornography. The affiant did not claim otherwise–he merely concluded, based upon information articulated in the warrant and his training and experience, that it was "extremely unlikely." Dkt. 47, Ex. 1, p. 12-13, ¶ 10. And even accepting Michaud's premise, which is not supported by the actual facts of the case, that contention does not defeat probable cause. As noted above, establishing probable cause does not require the negation of every alternate inference that could be drawn from the facts. Rather, an analysis of the totality of the circumstances, including reasonable inferences, counsels that the warrant was sufficiently supported by probable cause.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

3. The Affidavit Did Not Contain False or Misleading Statements Regarding the Location of the Search.

Michaud also baselessly contends that the affidavit included false and misleading statements regarding the location of the NIT search. According to Michaud, the warrant stated that the search would occur in the Eastern District of Virginia while in reality the search occurred on computers throughout the United States (indeed, the world), including computers within the Western District of Washington. Michaud is wrong. As detailed below, the warrant made clear that the NIT would be deployed in the Eastern District of Virginia, but that it would obtain information from computers that logged into Website A—the server for which was in the Eastern District of Virginia—wherever they may be located. He fails to support that argument with any offer of proof, affidavits or sworn or otherwise reliable statements to show any intentional or misleading statements, much less statements that are material to probable cause. Rather, the argument is based entirely on the defendant's own selective misleading reading of the NIT warrant, application, affidavit and attachments. No *Franks* hearing is warranted, or necessary, to dispose of this argument. The warrant paperwork contained a detailed and specific explanation of the NIT, indicating why its use was necessary, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.

The warrant application and warrant are captioned "in the matter of the search of computers that access [the URL of Website A]." Attachment A to the warrant specified that:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia. The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The affidavit made absolutely clear that the location of the activating computers was unknown, the NIT would be deployed on the website, and that purpose of the NIT warrant was to identify information about the location of activating computers. For instance, it articulated that without the use of the NIT "the identities of the administrators and users of [Website A] would remain unknown" because any IP address logs of user activity on Website A would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." Dkt. 47, Ex. 1, p. 22, ¶ 29. Further, the affiant concluded that "using a NIT may help FBI agents locate the administrators and users" of Website A. *Id*., pp. 23-24, ¶¶ 31-32. The affiant articulated that, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Website A users who were "engaging in the federal offenses enumerated" in the warrant. *Id*., p. 23, ¶ 31. Moreover, the affidavit specifically requested authority for the NIT to "cause an activating computer–wherever located–to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." *Id*., pp. 29-30, ¶ 46(a).

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of Website A that would be downloaded through normal operation of the site. *Id.*, p. 24, ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. *Id*. The exact information to be collected about was detailed in the warrant and accompanying Attachment A, along with technical explanations of the terms. It included the following: (1) an IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) an operating system; (4) information about whether the NIT had already been delivered; (5) a Host Name; (6) an active operating system username; and (7) a Media Access Control (MAC) address. *Id*., pp. 24-25, ¶ 34. The affidavit explained exactly why the information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." *Id*.,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

p. 26, ¶ 35. *Id*. The affidavit specifically requested authority to deploy the NIT to any user who logged into Website A with a username and a password. *Id*., p. 26, ¶ 36. Accordingly, a fair reading of the NIT warrant, application, affidavit and attachments made the location and object of the search eminently apparent. Michaud therefore fails to carry his burden of showing material misrepresentations or omissions that would defeat probable cause.

C. The NIT Warrant is Sufficiently Particular, and Therefore Not an Unconstitutional "General Warrant"

Michaud next claims that the NIT authorization constituted an unconstitutional "general warrant," essentially because it authorized, upon finding of probable cause, the collection of a limited set of particular, specified information from multiple computers. His argument misconstrues the Fourth Amendment concepts of particularity and scope, and is unavailing. Because the NIT authorization was founded on a sufficient showing of probable cause and specified, with particularity, the computers to which it applied and the exact, limited set of information to be seized, it did not constitute a unconstitutional "general warrant."

The Fourth Amendment states that "no warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV. It requires that two things be stated with particularity: "'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006). The place to be searched must be "described with sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort." *United States v. Turner*, 770 F.2d 1508, 1510 (9th Cir. 1985) (citations and quotations omitted). As for the items to be seized, a warrant is sufficiently particularized if "nothing is left to the discretion of the officer executing the warrant" regarding the choice of what to seize. *Marron v. United States*, 275 U.S. 192, 196 (1927). Whether this particularity standard is met is determined in light of the information available at the time the warrant issued. *United States v. Shi*, 525 F.3d 709, 731-32 (9th Cir. 2008).

Further, the Fourth Amendment requires that "the scope of what may be seized under the warrant be limited by the probable cause on which the warrant is based." *United States v. Brobst*, 558 F.3d 982, 993 (9th Cir. 2009) (emphasis added). "[T]he scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

that it may be found.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Indeed, "it is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant." *United States v. Gomez-Soto*, 723 F.3d 649, 654 (9th Cir. 1984). Thus, the concept of scope for Fourth Amendment purposes pertains to the relationship between the items to be seized pursuant to the warrant and the places in which those items are searched for–i.e., is it reasonable to look for the items to be seized, in the place being searched.

Applying these concepts here, the NIT warrant was sufficiently particular to comply with the Fourth Amendment. Attachments A and B of the NIT warrant, entitled "Place to be Searched," and "Information to be Seized," described with precise language exactly what would be searched and seized–the warrant authorized the NIT to be deployed on the computer server hosting Website A, in order to obtain specific information from computers of "any user or administrator who logs into [Website A] by entering a username and password." Dkt. 47, Ex. 1, Att. A. That specific information was detailed in Attachment B, and included: the computer's actual IP address, and the date and time that the NIT determines what that IP address is; a unique identifier generated by the NIT to distinguish data from that of other computers; the type of operating system running on the computer; information about whether the NIT has already been delivered to the "activating" computer; the computer's Host Name; the computer's active operating system username; and the computer's media access control ("MAC") address. *Id*., Att. B. Given these circumstances, there was no risk that the FBI would have trouble locating and identifying the location to be searched, or the information to be seized, and therefore no violation of the particularity requirement.

Michaud contends that the warrant was an unconstitutional "general" warrant because it applied to multiple computers. But the scope and particularity requirements of the Fourth Amendment place no such limits on the potential number of applicable locations to be searched, provided that the search of each location is supported by probable cause. Here, law enforcement sought and obtained a warrant to deploy the NIT to registered users who logged into the website. The warrant affidavit explained why it was reasonable to conclude that registered users of Website A were seeking child pornography, and Michaud has not directly challenged the

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

probable cause showing, apart from his *Franks* argument. Further, use of the NIT to identify an extremely limited set of information that would help identify those users was reasonable under the circumstances, given the targeted users deployment of anonymizing technology in order to illicitly exploit children. That there was probable cause to deploy the NIT against numerous criminal users of Website A was merely a result of the large number of criminal suspects under investigation, not of any constitutional infirmity in the particularity or scope of the warrant.

Moreover, the scope of the court-authorized NIT warrant–under a proper view of that concept–was actually extremely limited. Establishing probable cause to believe that Website A users were engaging in child pornography crimes would furnish sufficient cause to search the full content of any computer at such a user's residence for evidence such crimes. *See United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (warrant permitting seizure of Hay's "entire computer system and virtually every document in Hay's possession" for child pornography was proper); *United States v. Banks*, 556 F.3d 967, 974 (9th Cir. 2009) (warrant permitting search of all the defendant's computers for child pornography sufficiently particular); *United States v. Lacy*, 119 F.3d 742 at 746 (9th Cir. 1997) (blanket seizure and search of computer system for child pornography permitted). Yet the NIT search was infinitely narrower in scope than those sorts of warrants–collecting only a limited set of information to assist in identifying users who accessed Website A. The NIT did not authorize or conduct a full search of the contents of a user's computer or even the collection of the content of any communications. It merely collected a small set of information to assist in identifying the user and computer who accessed Website A–precisely the sort of information that would have been ordinarily been available to law enforcement (via website IP address logs) without need for the NIT authorization, had Website A been an ordinary website. Moreover, the key piece of evidence collected by the NIT–IP address information–is information that belongs to an internet service provider, not a user, and in which users do not have a reasonable expectation of privacy. Accordingly, the scope of the information collected via the NIT was amply tied to the probable cause established.

Nor did the fact that the location of user's computers was unknown at the time of the authorization render the search "general" or unreasonable. "The prohibition of general searches is not . . . a demand for precise *ex ante* knowledge of the location and content of evidence . . . . The proper metric of sufficient specificity is whether it was reasonable to provide a more specific

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

description of the items at that juncture of the investigation." *United States v. Banks*, 556 F.3d 967, 973 (9th Cir. 2009) (quoting *United States v. Meek*, 366 F.3d 705, 716 (9th Cir. 2004) (citation omitted). Here, as articulated to the issuing magistrate, users' locations were unknown due to their use of the Tor network, and the purpose of the search authorization was to obtain information that would assist in locating them. The use of the NIT for that purpose was eminently reasonable under those circumstances.

Michaud also points out that the NIT affidavit advised the issuing magistrate that, although the FBI requested (and was granted) authorization to deploy the NIT to any user who logged into Website A, in executing the warrant, the FBI might deploy the NIT more discretely against particular users who had attained higher status on the website or in particular areas of Website A containing the most egregious examples of child pornography. Dkt. 47, Ex. 1, p. 24 n. 8. While it was certainly reasonable for the affiant to advise the issuing magistrate that the FBI might execute the warrant on a smaller number of user computers than the warrant authorized, this articulation does not indicate a lack of particularity in the warrant. A warrant is sufficiently particularized if "nothing is left to the discretion of the officer executing the warrant" regarding the choice of what to seize. *Marron v. United States*, 275 U.S. 192, 196 (1927). A warrant is "facially deficient" only where it fails to provide any meaningful instruction to the searching agents regarding the items to be seized and "instead leaves the guessing as to their task." *United States v. Towne*, 997 F.2d 537, 549 (9th Cir. 1993). Here, the warrant authorized particular, specified information to be collected from specified users who logged in to the site with a username and password. Although the FBI retained discretion to execute the warrant on a narrower category of users than they were authorized to do so, nothing was left to law enforcement's discretion regarding what would be seized pursuant to the warrant.

Michaud briefly suggests that the FBI searched the "wrong" computer because the NIT collected information from his computer, as opposed to the website server. Dkt. 65, p. 15. This argument ignores the Court's authorization. Attachment A to the warrant specified that:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.
>
> The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.

The authorization plainly permitted the NIT to be deployed on the Website A computer server in order to collect the specified information from computers of users who logged into the website.

Finally, while the government may not have had probable cause to search Michaud's computer at the time the warrant was issued, though he was already at that time a registered user of Website A, that fact is of no moment as the NIT sufficed as a constitutional "anticipatory warrant." The Supreme Court, agreeing with all Courts of Appeals to address the issue, affirmed the constitutionality of these warrants in *United States v. Grubbs*, 547 U.S. 90 (2006):

> Anticipatory warrants are . . . no different in principle from ordinary warrants. They require the magistrate to determine (1) that it is now probable that (2) contraband, evidence of a crime, or a fugitive will be on the described premises (3) when the warrant is executed. . . . [T]wo prerequisites of probability must be satisfied. It must be true not only that if the triggering condition occurs "there is a fair probability that contraband or evidence of a crime will be found in a particular place," [*Illinois v. Gates*, 462 U.S. 213, 238 (1983)], but also that there is probable cause to believe the triggering condition will occur. The supporting affidavit must provide the magistrate with sufficient information to evaluate both aspects of the probable-cause determination."

Id. at 96-97. Here, to the extent necessary, the NIT affidavit amply supported both of those aspects of a probable cause determination. Attachments A and B, which were incorporated into the warrant, specified the exact conditions under which the NIT was authorized to be deployed–i.e., when a user such as Michaud logged in with a username and password to the website located in EDVA—and as discussed, there was probable cause to believe that any user who logged onto Website A was seeking child pornography. *See* Dkt. 47, Ex. 1, Att. A and B.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

D. The Good Faith Exception Applies to Bar Suppression Here.

Under the good faith exception to the exclusionary rule, suppression is not warranted where officers rely in good faith on an objectively reasonable search warrant issued by a neutral and detached judge. *United States v. Leon*, 468 U.S. 897, 900 (1984). This objective standard is measured by "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate judge's authorization." *Id.* at 922 n.23. The Supreme Court observed that "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion would further the purposes of exclusionary rule." *Id.* at 918. As such, the Court identified only four circumstances where exclusion is appropriate. Those are where: (1) the issuing magistrate was misled by the inclusion of knowing or recklessly false information; (2) the issuing magistrate wholly abandoned the detached and neutral judicial role; (3) the warrant is facially deficient as to its description of the place to be searched or the things to be seized; or (4) the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely upon it in good faith. *Id.* at 923-26. None apply here.

As argued herein, the warrant affidavit contained no knowing or recklessly false information that was material to the issue of probable cause. Michaud does not allege that the issuing magistrate abandoned her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. And the affidavit made a strong, comprehensive showing of probable cause to deploy the requested NIT. Ultimately, agents acted reasonably in relying upon the magistrate's authorization of the NIT warrant, and so the evidence seized pursuant to it should not be suppressed.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

IV. CONCLUSION

For all the foregoing reasons, the Court should deny Michaud's motion to suppress and request for a *Franks* hearing.

DATED this 21st day of December, 2015.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Andre M. Penalver
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail: matthew.hampton@usdoj.gov
andre.penalver@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on December 21, 2015, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

/s/ Matthew P. Hampton
MATTHEW P. HAMPTON
Assistant United States Attorney

E-mail: Lisa.Crabtree@usdoj.gov

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800